Identifying Enterprise Intrusion

A. Miller
Distinguished Professor of Electrical and Computer Engineering
University of Missouri-Rolla
125 Emerson Electric Co. Hall
Rolla, MO 65409-0040
United States

In the interests of readability and understandability, it is RTO policy to publish PowerPoint presentations only when accompanied by supporting text. There are instances however, when the provision of such supporting text is not possible hence at the time of publishing, no accompanying text was available for the following PowerPoint presentation.

Click here to view PowerPoint presentation; Press Esc to exit

Discussion – Paper 20

Bill Wright—scalability problem, data mining—finding the very few problems that really represent attacks
Dealing with False positives
MIT Bottleneck ID technique—try to characterize normal information flows of the enterprise, rather than characterize what attack would look like
Objection that still have false positives
Bayesian or neural models to distinguish between what is really unusual and what is normal traffic
Sharing the raw data in intrusion detection not done—trust the partner to perform their part of the interpretation correctly
Taxonomy (Kunar-session chair) problems with large data sets?
Milan—says uses an ontology approach
Seems to be some confusion w.r.t. use of terms "visualisation" vs. "taxonomy" vs. "ontology"
Portals—customized interfaces
Use one window to access all types of information/applications

Paper presented at the RTO IST Workshop on "Multimedia Visualization of Massive Military Datasets", held in Quebec, Canada, 6-9 June 2000, and published in RTO-MP-050.